UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

RAH-NITA BOYKIN and JESSICA SMITH,

Plaintiffs,

v.

LOANDEPOT, INC.,

Defendant.

Case No.: 1:24-cv-2583

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

TABLE OF CONTENTS

Plaintiffs Rah-Nita Boykin ("Plaintiff Boykin") and Jessica Smith ("Plaintiff Smith") (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, by and through their attorneys, bring this action against loanDepot, Inc. ("loanDepot," "LDI," or "Defendant") and allege, upon their personal knowledge and as to their own actions and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Corporations that collect consumers' sensitive information, including their names, phone numbers, addresses, email addresses, dates of birth, financial account numbers, Social Security numbers and/or passport numbers ("Personally Identifiable Information" or "PII"), have a duty to the consumers to protect their valuable, sensitive information.

2. Defendant is a publicly-traded nonbank holding company that sells mortgage and non-mortgage lending products, generating $974 million in revenue for 2023. As a corporation whose bread and butter requires the gathering of highly sensitive consumer financial information, Defendant is well aware of the life-altering impact a data breach can wreak on the average loanDepot customer or applicant.

3. Despite Defendant's status as a sophisticated, financial behemoth, Defendant failed to properly protect customers and applicants by investing in adequate data security, thereby allowing hackers to exfiltrate the highly-sensitive PII that customers entrusted to Defendant through various loan applications and loan services. Between January 3, 2024 and January 5, 2024, Defendant's failure to safeguard customer data resulted in a catastrophic, widespread data breach in which the data of 16.9 million customers was breached and exfiltrated (the "Data Breach").

4. On January 8, 2024, in a Form 8-K filing with the Securities and Exchange Commission ("SEC"), loanDepot reported it "recently identified a cybersecurity incident affecting

certain of the Company's systems."[1] Defendant later reported, as a result of the Data Breach, highly sensitive PII was accessed and exfiltrated by hackers, including names, phone numbers, email addresses, postal addresses, dates of birth, Social Security numbers, and financial account numbers.

5. Despite the highly sensitive nature of the personal information Defendant collected, and the prevalence of data breaches impacting financial institutions, Defendant inexplicably failed to implement and maintain reasonable and adequate security procedures and practices to safeguard the PII of Plaintiffs and the Class. The Data Breach itself and information Defendant has disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, and the sensitive nature of the impacted data, collectively demonstrate Defendant failed to implement reasonable measures to prevent the Data Breach and the exposure of highly sensitive customer information.

6. Defendant knew or should have known of the serious risk of harm caused by a data breach, including the importance of acting swiftly to protect PII. Yet, Defendant waited more than a month to begin notifying individuals impacted by the Data Breach, mailing out notices on February 26, 2023.

7. Defendant's failure to promptly notify Plaintiffs and Class members that their PII was exfiltrated due to Defendant's security failures virtually ensured that the unauthorized third parties who exploited Defendant's security vulnerabilities could monetize, misuse, and/or disseminate that PII before Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from

[1] https://investors.loandepot.com/financials/sec-filings/default.aspx (last accessed March 31, 2024).

the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated even beyond the Data Breach itself.

8. Plaintiffs and Class members had a reasonable expectation and understanding that Defendant would adopt adequate data security safeguards to protect their PII.

9. However, Defendant failed to: take sufficient and reasonable measures to safeguard its data security systems and protect highly sensitive data to prevent the Data Breach from occurring; to disclose to current and former customers or applicants the material fact that it lacked appropriate data systems and security practices to secure PII; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Because of Defendant's failures, Plaintiffs and Class members suffered substantial harm and injury.

10. As a direct result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common law obligations, Plaintiffs' and Class members' PII was accessed and acquired by unauthorized third parties for the purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of Defendant's current and former customers and applicants.

11. Plaintiffs and Class members face the real, immediate, and likely danger of identity theft and misuse of their PII, especially because their PII was specifically targeted by malevolent actors. Plaintiffs and Class members have a continuing interest in ensuring that their information is and remains safe.

12. Plaintiffs and Class members suffered injuries as a result of Defendant's conduct, including, but not limited to: lost of diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or

unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change usernames and passwords on their accounts; time needed to investigate, correct, and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect its PII. These risks will remain for the lifetimes of Plaintiffs and the Class.

13. Plaintiffs bring this action individually and on behalf of the Class, seeking relief including, but not limited to, compensatory damages, statutory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorneys' fees and costs, and all other remedies this Court deems proper.

II. PARTIES

14. Plaintiff Boykin is and has been at all relevant times a citizen and resident of Country Club Hills, Illinois.

15. Plaintiff Smith is and has been at all relevant times a citizen and resident of Denver, Colorado.

16. Defendant is a corporation organized under the laws of Delaware with a corporate headquarters, or principal place of business, located in Irvine, California.

III. JURISDICTION

17. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of costs and interest. At least one member of the Class is a citizen of a different state than Defendant, and there are more than 100 putative Class members.

18. Venue is proper in this judicial district under 28 U.S.C. § 1391 because Defendant transacts substantial business in this district, and because a substantial portion of the events giving rise to Plaintiff Boykin's claims occurred here.

19. This Court has personal jurisdiction over Defendant by virtue of its transactions and business conducted in this judicial district. For example, loanDepot maintains several branches in Illinois, where it employs loan consultants, a VP of Regional Production, and loan specialists, including but not limited to a Lincoln Park branch, a Pilsen branch, and a Beverly branch in Chicago, Illinois, and multiple Chicago-area suburban branches.[2] loanDepot also maintains a P.O. Box in Chicago where it accepts payments by customers for their home loans.[3] Defendant has transacted and done business, and violated statutory and common law, in the State of Illinois and in this judicial district.

IV. FACTUAL BACKGROUND

A. Background

20. Since its founding in 2010, Defendant has risen quickly to become one of the nation's largest non-bank mortgage lenders, "funding more than $275 billion since inception,"

[2] *See, e.g.,* https://www.loandepot.com/branches/chicago-il (last accessed April 1, 2024).

[3] *See* https://www.loandepot.com/about/loan-servicing (last accessed April 1, 2024).

through a team of "6,000-plus members" that assist more than 27,000 customers each month.[4] Defendant offers various home purchase, home refinance, and home equity loans.

21. Defendant touts itself as having "pioneered a digital-first approach that makes purchasing or refinancing a home easier, faster, and less stressful."[5]

22. Plaintiffs and Class Members sought loan services from loanDepot or its financial affiliates and/or subsidiaries. As part of the loan application process, Defendant collected some of their most sensitive and confidential information, including, without limitation: name, email address, username, password, Social Security number, phone number, mailing address, financial information, tax information, credit history, credit score, employment information, drivers' license information, insurance information, marital status, and other personal and highly sensitive information a person might provide when trying to procure a mortgage or loan.

23. As a result, Defendant hosts a large repository of sensitive personal information maintained for its customers and received from both customers and applicants, including Plaintiffs and the Class.

B. Defendant's Privacy Policy

24. Defendant's Privacy Policy (the "Privacy Policy") is accessible on its website and clearly states, "loanDepot® values your patronage and protecting your confidential information is a priority. Our policies and procedures reinforce the fact that loanDepot strongly believes in protecting the confidentiality and security of the information we collect about you as a customer, potential customer, or former customer."[6]

---

[4] https://www.loandepot.com/about (last accessed March 31, 2024).

[5] *Id*.

[6] https://investors.loandepot.com/privacy-policy/default.aspx (last accessed March 31, 2024).

25. In relevant part, the Privacy Policy states:

- We have adopted policies and procedures designed to protect your personally identifiable information from unauthorized use or disclosure.

- We have implemented physical, electronic, and procedural safeguards to maintain confidentiality and integrity of the personal information in our possession and to guard against unauthorized access. These include among other things, procedures for controlling access to your files, building security programs and information technology security measures such as the use of passwords, firewalls, virus prevention and use detection software.

- We continue to assess new technology as it becomes available and to upgrade our physical and electronic security systems as appropriate.

- Our policy is to permit employees to access your personal information only if they have a business purpose for using such information, such as administering, providing or developing our products or services.

- Our policy, which governs the conduct of all of our employees, requires all employees to safeguard personally identifiable information about the consumers and customers we serve or have served in the past.

loanDepot Security Policy

loanDepot takes strong steps to safeguard your personal and sensitive information through industry standard physical, electronic and operational policies and practices. All data that is considered highly confidential data can only be read or written through defined service access points, the use of which is password-protected. The physical security of the data is achieved through a combination of network firewalls and severs with tested operating systems, all housed in a secure facility. Access to the system, both physical and electronic, is controlled and sanctioned by a high-ranking manager.[7]

26. Based on these policies and representations, Defendant owed Plaintiffs and the Class a duty to protect their privacy and safeguard the sensitive personal information and PII of its current and former customers and applicants.

C. The Data Breach

27. From approximately January 3, 2024 through January 5, 2024, a malicious actor gained unauthorized access to Defendant's company data systems, including the sensitive

[7] *Id.*

personal, financial, and other confidential information of loanDepot's potential, former, and current customers like Plaintiffs and the Class.[8]

28. Upon information and belief, the actors accessed and acquired substantial amounts of Plaintiffs' and the Class's sensitive personal information, including their PII. This data included highly sensitive personal information such as names, addresses, Social Security numbers, employment information, and financial account numbers information.

29. On January 8, 2024, Defendant posted the following to its website:

> LoanDepot is experiencing a cyber incident. We have taken certain systems offline and are working diligently to restore normal business operations as quickly as possible. We are working quickly to understand the extent of the incident and taking steps to minimize its impact. The Company has retained leading forensics experts to aid in our investigation and is working with law enforcement. We sincerely apologize for any impacts to our customers, and we are focused on resolving these matters as soon as possible.[9]

30. In a January 8, 2024 filing with the SEC, Defendant reported that "the Company has determined that the unauthorized third-party activity included access to certain Company systems and the encryption of data."[10]

31. Data breaches described as "encryption of data" are typically ransomware attacks in which third parties lock and encrypt a company's data, files, devices or systems, rendering them inaccessible and unusable until the attacker receives a ransom payment. Since the Data Breach, a ransomware gang known as AlphV/BlackCat has claimed credit for the attack.[11]

---

[8] https://cybernews.com/news/loandepot-finally-reveals-what-data-exposed-in-jan-hack/ (last accessed March 31, 2024).

[9] https://loandepot.cyberincidentupdate.com (last accessed March 31, 2024).

[10] https://d18rn0p25nwr6d.cloudfront.net/CIK-0001831631/446c437f-153f-425d-adc6-bf37155d6e91.pdf (last accessed March 31, 2024).

[11] https://www.housingwire.com/articles/alphv-blackcat-claims-credit-for-loandepot-cyberattack/ (last accessed March 31, 2024).

32. In a January 22nd update, Defendant posted the following:

> The Company has been working diligently with outside forensics and security experts to investigate the incident and restore normal operations as quickly as possible. The Company has made significant progress in restoring our loan origination and loan servicing systems, including our MyloanDepot and Servicing customer portals.
>
> Although its investigation is ongoing, the Company has determined that an unauthorized third party gained access to sensitive personal information of approximately 16.6 million individuals in its systems. The Company will notify these individuals and offer credit monitoring and identity protection services at no cost to them.
>
> "Unfortunately, we live in a world where these types of attacks are increasingly frequent and sophisticated, and our industry has not been spared. We sincerely regret any impact to our customers," said loanDepot CEO Frank Martell. "The entire loanDepot team has worked tirelessly throughout this incident to support our customers, our partners and each other. I am pleased by our progress in quickly bringing our systems back online and restoring normal business operations."
>
> "Our customers are at the center of everything we do," said Jeff Walsh, President of LDI Mortgage. "I'm really proud of our team, and we're glad to be back to doing what we do best: enabling our customers across the country to achieve their financial goals and dreams of homeownership."
>
> The Company is committed to keeping its customers, partners and employees informed and will provide any additional operational updates on our microsite at loandepot.cyberincidentupdate.com.[12]

33. On February 23, 2024, Defendant reported to Maine's Attorney General's office that nearly 17 million people were impacted by the data breach and that impacted data included name, address, email address, financial account numbers, Social Security number, phone number, and date of birth.[13]

[12] https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx (last accessed March 31, 2024).

[13] https://apps.web.maine.gov/online/aeviewer/ME/40/2b910ff6-9bd0-4fcf-a766-cd2c0bc85dec.shtml?1708971900 (last accessed March 31, 2024).

D. Defendant's Failures Prior to and Following the Data Breach

34. Defendant knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

35. In fact, Defendant is no stranger to the dangers posed by storing sensitive PII because it suffered a data breach via phishing attack in August 2022.[14] Despite Defendant's claims that it took immediate action for the August 2022 attack, Defendant did not disclose the breach until nearly a year later on April 24, 2023.[15]

36. Ransomware attacks like the Data Breach here are frequently used to target companies due to the volume of sensitive data that they collect, maintain, and store.[16] From 2022 to 2023, statistics show more than a 73% increase[17] in ransomware attacks, resulting in more than $1.1 billion in ransomware payments.[18]

37. According to the Center for Internet Security, companies should treat ransomware attacks as any other data breach incident because ransomware attacks do not simply hold networks hostage and/or publicly disclose the data; rather, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[19]

---

[14] https://www.doj.nh.gov/consumer/security-breaches/documents/loandepot-20230424.pdf (last accessed March 31, 2024).

[15] *Id*.

[16] Charles Griffiths, *The Latest 2023 Cyber Crime Statistics (updated October 2023)*, AAG (Feb. 10, 2023).

[17] https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/ (last accessed March 31, 2024).

[18] https://www.chainalysis.com/blog/ransomware-2024/ (last accessed March 31, 2024).

[19] *Ransomware: The Data Exfiltration and Double Extortion Trends*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltrationanddouble-extortion-trends

38. Defendant could have prevented this Data Breach by properly encrypting or otherwise protecting its equipment and network files containing PII.

39. Despite widespread industry warnings, Defendant failed to implement and use reasonable security procedures and practices to protect Plaintiffs' and similarly situated individuals' sensitive PII.

40. Defendant's failure to properly safeguard Plaintiffs' and Class members' PII allowed the unauthorized actors to access this highly sensitive PII.

41. The Data Breach highlights the inadequacies inherent in Defendant's network monitoring procedures and security training protocols. If Defendant had properly monitored its cybersecurity systems and implemented a sufficient training protocol for its employees, it would have prevented the Data Breach, discovered the Data Breach sooner, and/or have prevented the hackers from accessing PII.

42. Moreover, when Defendant acknowledged that it was experiencing the breach, it failed to fully inform affected individuals of the length of time that the unauthorized actors had access to their PII, or the full extent of the PII that was accessed during the Data Breach.

43. Defendant's failure to timely notify Plaintiffs and other victims of the Data Breach that their PII had been misappropriated precluded them from taking meaningful steps to safeguard their identities prior to the dissemination of their PII.

44. Defendant's delayed response only further exacerbated the consequences of the Data Breach brought on by its systemic IT failures.

45. Defendant's failures are three-fold. First, Defendant failed to timely secure its computer systems to protect its current and former customers' and applicants' PII. Defendant

allowed the unauthorized actors to continue to have unfettered access to Defendant's systems for at least two days until Defendant finally secured its systems.

46. Second, Defendant failed to timely notify affected individuals, including Plaintiffs and Class members, that their highly sensitive PII had been accessed by unauthorized third parties. Despite knowing that a cybersecurity issue had occurred at least as early as January 4, 2024, Defendant waited until February 23, 2024, to provide notice to the victims of the Data Breach that their PII had been compromised.

47. Third, Defendant made no effort to protect Plaintiffs and the Class from the long-term consequences of Defendant's acts and omissions. Although the Notice offered victims complimentary credit monitoring and fraud assistance services, Plaintiffs' and Class members' PII, including their Social Security numbers, cannot be changed and will remain at risk long beyond two years. As a result, Plaintiffs and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

48. In short, Defendant's myriad failures, including the failure to timely detect the Data Breach and to notify Plaintiffs and the Class with reasonable timeliness that their PII had been accessed due to Defendant's security failures, allowed unauthorized individuals to access and misappropriate Plaintiffs' and Class members' PII for more than a month before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

E. Data Breaches Pose Significant Threats to Consumers

49. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors and lead to considerable costs to consumers. According to Statista, during the first quarter of 2023 alone, more than six million data records were exposed

worldwide through data breaches.[20] Indeed, cybercrime is slated to cost the world $10.5 trillion annually by 2025.[21]

50. Identity theft is the most common consequence of data breaches to consumers. A 2021 report concluded that more than half of all data breaches resulted in identity theft, including unauthorized access to a victim's financial accounts, opening new accounts in the victim's name, and using a victim's personal information for other fraudulent activities.[22]

51. As a result, consumers' PII is an invaluable commodity and the most frequent target of hackers.[23] Numerous sources cite dark web pricing for personal information, such as name, date of birth, and Social Security number, ranging from $40 to $200.[24]

52. Many tend to minimize the value of certain categories of PII, such as names, birthdates, addresses, and phone numbers. However, security experts agree that "[i]f you have someone's name and address, that is still valuable."[25] At the end of the day, "the more info you have, the more it is worth."[26]

53. Thefts of Social Security numbers present an even greater risk to consumers. Indeed, data breaches involving Social Security numbers are "incredibly alarming" because

---

[20] *Number of data records exposed worldwide from 1st quarter 2020 to 1st quarter 2023*, Statista (May 2023), *available at* https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/#:~:text=During%20the%20first%20quarter%20of,nearly%20125%20million%20data%20sets

[21] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, Cybercrime Magazine (Nov. 13, 2020).

[22] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019).

[23] *Id*.

[24] *Id*.

[25] Robert Lemos, *All about your 'fullz' and how hackers turn your personal data into dollars*, PCWorld (June 2, 2016).

[26] *Id.*

"[u]nlike a credit card number which can be changed, Social Security numbers . . . are hard to change, or cannot be changed."[27]

54. Even if victims whose Social Security numbers have been compromised are able to change their Social Security numbers, the new number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

55. Driver's license numbers are likewise incredibly valuable because they can be a critical part of a fraudulent, synthetic identity, which can sell for as much as $1,200 on the dark web.[29] Driver's license numbers alone sell for as much as $200.[30]

56. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[31] However, as cybersecurity experts point out, this is not the case: "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[32]

---

[27] Brian Naylor, *Victims Of Social Security Number Theft Find It's Hard To Bounce Back*, NPR (Feb. 9, 2015).

[28] *Id*.

[29] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customer to Watch Out for Fraudulent Unemployment Claims*, CPO Magazine (Apr. 23, 2021).

[30] *Id.*

[31] *Id*.

[32] *Id.*

57. Like victims of Social Security number theft, victims of driver's license number theft are also at risk of suffering unemployment benefit fraud, as highlighted by the New York Times.[33]

58. Theft of financial account numbers present serious and immediate consequences. Experian warns that "[i]f someone gains access to your bank account and routing numbers, they can use the information to fraudulently withdraw or transfer money from your account. They can also create fake checks, claim your tax return or commit other forms of financial fraud."[34]

59. Here, Plaintiffs and the Class face the threat of losing critical sums of money through fraudulent withdrawals from financial accounts, in addition to the long-term danger of identity theft.

60. According to the FTC, in 2021, around 20% of Americans were victims of identity theft, indicating that most Americans have either been a victim of identity theft or know someone who has.[35]

61. The fraudulent activity resulting from Defendant's Data Breach may not come to light for years, as there may be a time lag between when Plaintiffs' and Class members' PII was stolen and when it is used, meaning there may be a delay between when the harm occurs versus when it is discovered.[36]

---

[33] Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, New York Times (Apr. 27, 2021).

[34] https://www.experian.com/blogs/ask-experian/what-can-someone-do-with-your-bank-account-and-routing-numbers/ (last accessed March 31, 2024).

[35] *Consumer Sentinel Network Data Book 2021*, Federal Trade Commission (Feb. 2022) *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf (last accessed March 31, 2024).

[36] *Report to Congressional Requesters*, Government Accountability Office, at 29 (June 2007) *available at* https://www.gao.gov/assets/gao-07-737.pdf (last accessed March 31, 2024).

62. Beyond economic impacts, identity theft also leads to lasting emotional impacts; a majority of the victims of identity theft report increased stress levels, fatigue, and trust issues with family and friends and decreased energy.[37]

63. Given the nature of Defendant's Data Breach, as well as the delay in notification to Class members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways.

64. Despite the prevalence of public announcements of data breach and data security compromises, as well as the risks posed by compromises of PII, Defendant failed to take proper action to protect the PII of Plaintiffs and the Class from misappropriation. As a result, the injuries to Plaintiffs and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measure for its customers.

F. Defendant Had a Duty and Obligation to Protect PII

65. Defendant has an obligation to keep confidential and protect from unauthorized access and/or disclosure Plaintiffs' and Class members' PII. Defendant's obligations are derived from: 1) government regulations and state laws, including FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII. Plaintiffs and Class members provided—and Defendant obtained—their PII on the understanding that their PII would be protected and safeguarded from unauthorized access or disclosure.

66. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[38] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other

[37] *New Study by Identity Theft Resource Center Explores the Non-Economic Negative Impacts Caused by Identity Theft*, Identity Theft Resource Center (Oct. 18, 2018).

[38] 17 C.F.R. § 248.201.

information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

67. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices, explaining that the need for data security should be factored into all business decision-making.[39]

68. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for businesses.[40] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[41] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[42] Defendant clearly failed to do any of the foregoing, as evidence by the Data Breach and amount of data accessed.

---

[39] *See* Start with Security, Federal Trade Commission (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[40] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[41] *Id*.

[42] *Id*.

69. Here, at all relevant times, Defendant was fully aware of its obligation to protect the PII of its current and former customers and applicants, including Plaintiffs and the Class. Defendant is a sophisticated, technologically-savvy, multi-billion-dollar, publicly-traded financial services company that relies extensively on technology systems to operate its business, including transmitting its customers' and applicants' PII over those systems.

70. Defendant had, and continues to have, a duty to exercise reasonable care in collecting, storing, and protecting PII from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and Plaintiffs and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cybersecurity network to secure and protect Plaintiffs' and Class members' PII.

71. Defendant's failure to follow the FTC guidelines and its subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data constitutes unfair acts or practices prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

72. Further, Defendant had a duty to promptly notify Plaintiffs and the Class that their PII was accessed by unauthorized persons.

G. Defendant's Conduct Violated the FTC Act & Industry Standards for Safeguarding Customers and Applicants' PII

73. The FTC rules, regulations, and guidelines obligate businesses to protect PII from unauthorized access or disclosure by unauthorized persons.

74. At all relevant times, Defendant was fully aware of its obligation to protect its customers' and applicants' PII because it is a sophisticated business entity that is in the business of maintaining and transmitting PII.

75. Defendant was also aware of the significant consequences of its failure to protect the PII of its customers and applicants and knew that this data, if hacked, would injure individuals, including Plaintiffs and Class members.

76. Defendant failed to comply with FTC rules, regulations, and guidelines and industry standards concerning the protection and security of PII. As evidenced by the duration, scope, and nature of the Data Breach, among its many deficient practices, Defendant failed in, *inter alia*, the following respects:

a. Developing and employing adequate intrusion detection systems;
b. Engaging in regular reviews of audit logs and authentication records;
c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;
d. Ensuring the confidentiality and integrity of current and former customers and applicants' PII;
e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of its current and former customers and applicants' PII;
f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;
g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;
h. Implementing technical policies, procedures, and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access; and

i. Other similar measures to protect the security and confidentiality of its current and former customers or applicants' PII.

77. Had Defendant implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Defendant could have prevented or detected the Data Breach prior to the hackers accessing Defendant's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former customers or applicants of Defendant would have been notified sooner, allowing them to promptly take protective and mitigating actions.

H. Defendant's Data Security Practices are Inadequate and Inconsistent with its Self-Imposed Data Security Obligations

78. Defendant purports to care about data security and safeguarding customers' and applicants' PII and represents that it will keep secure and confidential the PII belonging to its current and former customers or applicants.

79. Plaintiffs' and Class members' PII was provided to Defendant in reliance on its promises and self-imposed obligations to keep PII confidential and to secure the PII from unauthorized access by malevolent actors. Defendant failed to do so.

80. Had Defendant undertaken the actions that federal and state law require, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as Defendant would have thwarted hackers' access to its systems in the first instance or otherwise detected the Data Breach prior to the hackers accessing data from Defendant's networks, and Defendant's current and former customers or applicants would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

81. Indeed, following the Data Breach, Defendant effectively conceded that its security practices were inadequate and ineffective. In the Notice it sent to Plaintiffs and others, Defendant acknowledged that the Data Breach required it to hire "outside forensics and security experts" to assist with its investigation into the Data Breach and "tak[e] steps to minimize its impact."[43]

82. Like any data hack, the Data Breach presents major problems for all affected. According to Jonathan Bowers, a fraud and data specialist at fraud prevention provider Trustev, "Give a fraudster your comprehensive personal information, they can steal your identity and take out lines of credit that destroy your finances for years to come."[44]

83. The FTC warns the public to pay particular attention to how they keep personally identifying information, including Social Security measures and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[45]

84. According to data security experts, one out of every three data breach notification recipients becomes a victim of identity fraud.[46]

85. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

---

[43] https://loandepot.cyberincidentupdate.com/ (last accessed March 31, 2024).

[44] Roger Cheng, *Data breach hits roughly 15M T-Mobile customers, applicants*, CNET (Oct. 1, 2015).

[45] *Warning Signs of Identity Theft*, Federal Trade Commission, *available at* https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed Nov. 8, 2023).

[46] *A New Identity Fraud Victim Every Two Seconds in 2013 According to Latest Javelin Strategy & Research Study*, Javelin Strategy & Research (Feb. 5, 2014), *available at* https://javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy.

86. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[47] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[48] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has yet to be exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class members' PII will do so at a later date or re-sell it.

87. In response to the Data Breach, Defendant offered to provide certain individuals whose PII was exposed in the Data Breach with two years of credit monitoring. However, two years of complimentary credit monitoring cannot adequately protect against the lifelong risk of harm imposed on Plaintiffs and Class members by Defendant's failures.

88. Moreover, the credit monitoring offered by Defendant is inadequate to protect Plaintiffs and Class members from the injuries resulting from the unauthorized access of their sensitive PII.

89. Due to the Breach, Plaintiffs and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of their PII;

[47] Susan Ladika, *Study: Data Breaches Pose a Greater Risk*, Fox Business (July 28, 2014), *available at* https://www.foxbusiness.com/features/study-data-breaches-pose-a-greater-risk.

[48] Al Pascual, *The Consumer Data Insecurity Report*, Javelin Strategy & Research (June 30, 2014), *available at* https://javelinstrategy.com/research/consumer-data-insecurity-report.

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the PII stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all these issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their PII is exposed for theft and sale on the dark web; and

f. The loss of Plaintiffs' and Class members' privacy.

90. Plaintiffs and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII being accessed by cybercriminals, risks that will not abate within a mere two years: the unauthorized access of Plaintiffs' and Class members' PII, especially their Social Security numbers, puts Plaintiffs and the Class at risk of identity theft indefinitely, and well beyond the

limited period of credit monitoring that Defendant offered victims of the Breach. The two years of credit monitoring that Defendant offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiffs and Class members have suffered and will continue to suffer as a result of the Data Breach.

91. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure PII, Plaintiffs and Class members have been placed at a substantial risk of harm in the form of identity theft and have incurred and will incur actual damages in an attempt to prevent identity theft.

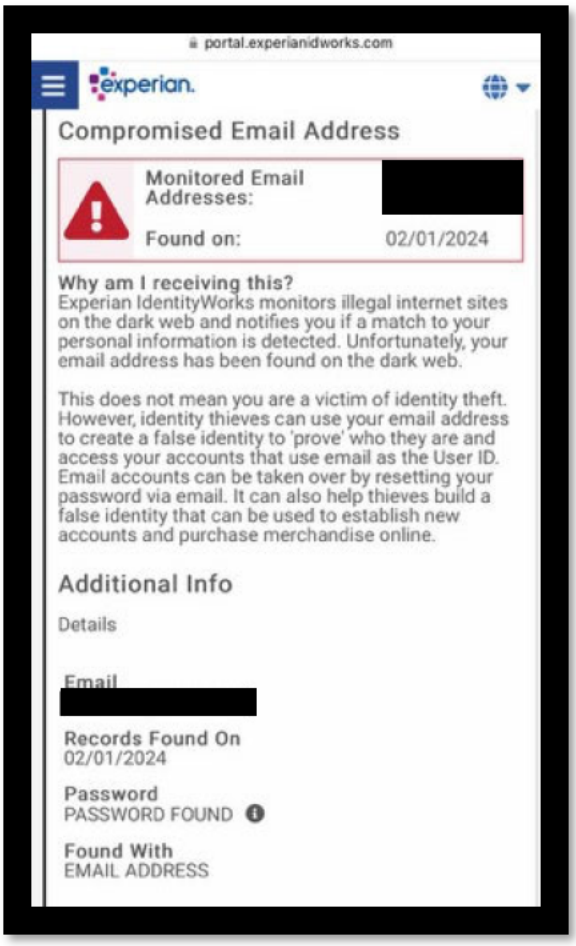
92. Plaintiffs retain an interest in ensuring there are no future breaches, especially given Defendant suffered a separate data breach event as recently as 2022, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of themselves and similarly situated individuals whose PII was accessed in the Data Breach.

93. Defendant is aware of the ongoing harm that the Data Breach has and will continue to impose of Defendant's current and former customers and applicants, as the notices it posted and sent to Plaintiffs and Class members regarding the Data Breach advise victims to "remain vigilant" in reviewing account statements and credit reports.[49]

I. Plaintiff Boykin's Experience

94. In February 2024, Plaintiff Boykin received a notification from Experian indicating that her information was detected on the dark web. Plaintiff Boykin was not aware of how her data had been compromised but began closely monitoring her accounts.

[49] *See* Notice, attached as Exhibit 1.



95. In approximately early March 2024, Plaintiff Boykin received a notice from Defendant that her PII had been compromised in the Data Breach and improperly obtained by third parties. The notice indicated that Plaintiff Boykin's PII, including her name, phone number, email address, postal address, date of birth, Social Security number, and financial account numbers were compromised in the Data Breach.

96. As a result of the Data Breach, Plaintiff Boykin has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services.

Plaintiff Boykin has spent valuable time dealing with the Data Breach, time Plaintiff Boykin otherwise would have spent on other activities, including work and/or recreation.

97. Following Plaintiff Boykin's receipt of Defendant's notice of Data Breach, Plaintiff Boykin noticed a significant increase in spam calls, text messages, and emails.

98. Plaintiff Boykin suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Boykin; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft; and (d) loss of benefit of the bargain.

99. As a result of the Data Breach, Plaintiff Boykin anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Boykin is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

J. Plaintiff Smith's Experience

100. In approximately mid-March 2024, Plaintiff Smith received a notice from Defendant that her PII had been compromised in the Data Breach and improperly obtained by third parties. The notice indicated that Plaintiff Smith's PII, including her name, phone number, email address, postal address, date of birth, Social Security number, and financial account numbers were compromised in the Data Breach.

101. As a result of the Data Breach, Plaintiff Smith has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services.

Plaintiff Smith has spent valuable time dealing with the Data Breach, time Plaintiff Smith otherwise would have spent on other activities, including work and/or recreation.

102. Plaintiff Smith suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Smith; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft; and (d) loss of benefit of the bargain.

103. As a result of the Data Breach, Plaintiff Smith anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Smith is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

104. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Nationwide Class defined as:

> **All persons in the United States whose PII was accessed in the Data Breach announced by Defendant on January 8, 2024 (the "Nationwide Class").**

105. Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change, or expand the Class definition after conducting discovery.

106. In addition, Plaintiff Boykin brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), an Illinois Subclass defined as:

> **All persons who are residents of the State of Illinois whose PII was accessed in the Data Breach announced by Defendant on January 8, 2024 (the "Illinois Subclass").**

107. Excluded from the Illinois Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

108. In addition, Plaintiff Smith brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Colorado Subclass defined as:

> **All persons who are residents of the State of Colorado whose PII was accessed in the Data Breach announced by Defendant on January 8, 2024 (the "Colorado Subclass").**

109. Excluded from the Colorado Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

110. The Nationwide Class, the Illinois Subclass, and the Colorado Subclass are collectively referred to herein as the "Class."

111. **Numerosity**: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiffs only through the discovery process, Plaintiffs believe, and on that basis allege, that at least 16,924,071 individuals' PII were affected by the Data Breach. The members of the Class will be identified through information and records in Defendant's possession, custody, and control.

112. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions including, but are not limited to:

a. Whether Defendant's data security and retention policies were unreasonable;

b. Whether Defendant failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether Defendant owed a duty to Plaintiffs and Class members to safeguard their PII;

d. Whether Defendant breached any legal duties in connection with the Data Breach;

e. Whether Defendant's conduct was intentional, reckless, willful, or negligent;

f. Whether an implied contract was created concerning the security of Plaintiffs' and Class members' PII;

g. Whether Defendant breached that implied contract by failing to protect and keep secure Plaintiffs' and Class members' PII and/or failing to timely and adequately notify Plaintiffs and Class members of the Data Breach;

h. Whether Plaintiffs and Class members suffered damages as a result of Defendant's conduct;

i. Whether Plaintiffs and the Class are entitled to monetary damages, injunctive relief, and/or other remedies and, if so, the nature of any such relief.

113. **Typicality**: Plaintiffs' claims are typical of the claims of the Class because Plaintiffs and all members of the Class were injured through Defendant's uniform misconduct. The actions and omissions that gave rise to Plaintiffs' claims are the same that gave rise to the claims of every other Class member because Plaintiffs and each Class member had their sensitive PII compromised in the Data Breach due to Defendant's misconduct, and there are no defenses that are unique to Plaintiffs.

114. **Adequacy**: Plaintiffs are adequate representatives because their interests do not conflict with the interests of the Class that they seek to represent, they have retained counsel

competent and highly experienced in complex class action litigation, and they intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

115. **Superiority**: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and members of the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based on Defendant's records.

116. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE

(On Behalf of Plaintiffs and the Class)

117. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

118. Defendant owed a duty to Plaintiffs and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII that Defendant collected.

119. Defendant owed a duty to Plaintiffs and the Class to provide security, consistent with industry standards and requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the PII that Defendant collected.

120. Defendant owed a duty to Plaintiffs and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

121. Defendant owed a duty of care to Plaintiffs and the Class because it was a foreseeable and probable victim of any inadequate data security practices.

122. Defendant solicited, gathered, and stored the PII belonging to Plaintiffs and the Class.

123. Defendant knew or should have known it inadequately safeguarded this information.

124. Defendant knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiffs and Class members, and Defendant was therefore charged with a duty to adequately protect this critically sensitive information.

125. Defendant had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' highly sensitive PII was entrusted to Defendant on the understanding that adequate security precautions would be taken to protect the PII. Moreover, only Defendant had the ability to protect its systems and the PII stored on them from attack.

126. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs, Class members, and their PII. Defendant's misconduct included failing to: (1) secure its systems, servers,

and networks, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement safeguards, policies, and procedures necessary to prevent this type of data breach.

127. Defendant breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the PII belonging to Plaintiffs and the Class.

128. Defendant breached its duties to Plaintiffs and the Class by creating a foreseeable risk of harm through the misconduct previously described.

129. Defendant breached the duties it owed to Plaintiffs and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII.

130. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII belonging to Plaintiffs and the Class so that Plaintiffs and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

131. Defendant breached the duties it owed to Plaintiffs and the Class by failing to disclose timely and accurately to Plaintiffs and Class members that their PII had been improperly acquired or accessed.

132. Defendant breached its duty to timely notify Plaintiffs and Class members of the Data Breach by failing to provide direct notice to Plaintiffs and the Class concerning the Data Breach until on or about February 23, 2024.

133. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before

the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

134. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II – NEGLIGENCE *PER SE*

(On Behalf of Plaintiffs and the Class)

135. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

136. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

137. The Illinois Consumer Fraud and Deceptive Business Practices Act ("Illinois Consumer Fraud Act"), 815 ILCS 505/1 et seq., prohibits unfair or deceptive acts or practices in the conduct of trade or commerce.

138. The Colorado Consumer Protection Act ("Colorado CPA") Colo. Rev. Stat. § 6-1-713.5 requires commercial entities who maintain, own, or license personal identifying information of an individual residing in the state of Colorado to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

139. In addition to the FTC rules and regulations, the Illinois Consumer Fraud Act, the Colorado CPA, and other states and jurisdictions where victims of the Data Breach are located require that Defendant protects PII from unauthorized access and disclosure, and timely notify the victim of a data breach.

140. Defendant violated the Illinois Consumer Fraud Act, Colorado CPA, and FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards, and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of the Data Breach, and the exposure of Plaintiffs' and Class members' sensitive PII.

141. Defendant's violations of the Illinois Consumer Fraud Act, Colorado CPA, FTC rules, and other applicable statutes, rules, and regulations constitutes negligence *per se*.

142. Plaintiffs and the Class are within the category of persons the Illinois Consumer Fraud Act, Colorado CPA, and the FTC Act were intended to protect.

143. The harm that occurred as a result of the Data Breach described herein is the type of harm the Illinois Consumer Fraud Act, Colorado CPA, and the FTC Act were intended to guard against.

144. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

COUNT III - BREACH OF CONTRACT

(On Behalf of Plaintiffs and the Class)

145. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

146. Plaintiffs and Class members entered into a valid and enforceable contract through which they were required to provide their PII to Defendant in exchange for services.

147. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class members' sensitive personal information to any third parties without their consent.

148. Defendant's promises and Plaintiffs and Class Members rights and obligations, are memorialized in loanDepot's privacy policy, published on its website. Defendant's privacy policy is part of Plaintiffs' and Class Members' agreement for services or application for services with loanDepot.

149. Plaintiffs and Class Members fully performed their obligations pursuant to their contracts with loanDepot. Defendant breached its contracts with Plaintiffs and Class Members when it failed to protect, secure, and/or keep private Plaintiffs' and Class Members' PII.

150. As a result, Plaintiffs and Class members have been harmed, damaged, and/or injured as described herein, including by Defendant's failure to fully perform its part of the agreement with Plaintiffs and Class members.

151. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV - BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs and the Class)

152. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

153. When Plaintiffs and Class Members provided their PII to Defendant, they entered into implied contracts with Defendant, under which Defendant agree to take reasonable steps to protect Plaintiffs' and Class Members' PII, comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PII, and to timely notify them in the event of a data breach.

154. Defendant solicited and invited Plaintiffs and Class Members to provide their PII as part of Defendant's provision of mortgage and lending services. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

155. Implicit in the agreement between Plaintiffs and Class Members and Defendant was Defendant's obligation to: (a) use such PII for business purposes only; (b) take reasonable steps to safeguard Plaintiffs' and Class Members' PII; (c) prevent unauthorized access and/or disclosure of Plaintiffs' and Class Members' PII; (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their PII; (e) reasonably safeguard and protect the PII of Plaintiffs' and Class Members from unauthorized access and/or disclosure; and (f) retain Plaintiffs' and Class Members' PII under conditions that kept such information secure and confidential.

156. Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

157. Plaintiffs and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

158. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

159. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard their PII and by failing to provide them with timely and accurate notice of the Data Breach.

160. The losses and damages Plaintiffs and Class Members sustained, include, but are not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Loss of money due to fraudulent withdrawals and fraudulent transfers from their financial accounts;

d. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

j. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

k. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

COUNT V - VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT (CONSUMER FRAUD ACT) (815 ILLINOIS COMPILED STATUTES 505/1 et seq.)

(On Behalf of Plaintiff Boykin and the Illinois Subclass)

161. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

162. The Illinois Consumer Fraud and Deceptive Business Practices Act ("Illinois Consumer Fraud Act"), 815 ILCS 505/1 et seq. declares unlawful "any . . . false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, . . . in the conduct of any trade or commerce . . . whether any person has in fact been misled, deceived or damaged thereby."

163. Plaintiffs and other members of the Illinois Subclass are "persons" within the meaning of 815 ILCS 505/1 § (1)(b).

164. Defendant's conduct alleged herein constitutes a "sale" within the meaning of 815 ILCS 505/1 § (1)(d) because Plaintiffs and the Class's data is now offered for sale on the dark web.

165. In the Privacy Policy, Defendant represented to Plaintiffs and the Class Members that their PII would be encrypted and/or securely maintained by virtue of security programs and information technology security measures such as the use of passwords, firewalls, virus prevention and use detection software.

166. By requiring Plaintiffs and Class Members to agree to Defendant's Privacy Policy, Defendant intended Plaintiffs and the Class Members to rely on it. The Privacy Policy represented that Plaintiffs' and Class Members' PII would be protected by Defendant. Plaintiffs and Class Members were required to agree to Defendant's Privacy Policy in order to apply for or use Defendant's services. Plaintiffs and Class Members relied on Defendant to protect and/or secure their PII per the Privacy Policy.

167. Defendant's misrepresentations and false, deceptive, and misleading statements and omissions with respect to its privacy policy as described above, constitute affirmative misrepresentations in violation of the Illinois Consumer Fraud Act.

COUNT VI – VIOLATION OF THE COLORADO CONSUMER PROTECTION ACT (Colo. Rev. Stat. § 6-1-713.5)

(On Behalf of Plaintiff Smith and the Colorado Subclass)

168. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

169. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

170. Colo. Rev. Stat. § 6-1-713.5 requires commercial entities who maintain, own, or license "personal identifying information of an individual residing in the state" to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

171. Defendant's conduct violated Colo. Rev. Stat. § 6-1-713.5. Specifically, Defendant voluntarily undertook the act of maintaining and storing Plaintiffs' PII but Defendant failed to implement safety and security procedures and practices sufficient enough to protect from the data breach that it should have anticipated. Defendant should have known and anticipated that data breaches—especially financial data—were on the rise, and that financial institutions were lucrative or likely targets of cybercriminals looking to steal PII. Correspondingly, Defendant should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the data breach.

172. As a result of Defendant's violation of Colo. Rev. Stat. § 6-1-716, Plaintiffs and the Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully request that the Court enter a judgment on their behalf and against Defendant loanDepot, Inc., and further grant the following relief:

A. Certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Designate Plaintiffs as representatives of the proposed Class and subclasses and Plaintiffs' counsel as Class counsel;

C. Grant Plaintiffs the declaratory relief sought herein;

D. Grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

E. Award Plaintiffs and the Class compensatory, consequential, and general damages in an amount to be determined at trial, and any other relief to which they are entitled under the law;

F. Award Plaintiffs and the Class statutory damages, and punitive or exemplary damages, to the extent permitted by law;

G. Award prejudgment interest, costs, and attorneys' fees;

H. Award all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. Award Plaintiffs and the Class such other and further relief as the Court deems just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiffs, individually and on behalf of the proposed Class, respectfully request a trial by jury as to all matters so triable.

Dated: April 1, 2024

Respectfully submitted,

By: */s/ Elizabeth A. Fegan*

Elizabeth A. Fegan
Megan E. Shannon
FEGAN SCOTT LLC
150 S. Wacker Drive, 24th Floor
Chicago, IL 60606
Telephone: (312) 741-1019
Facsimile: (312) 264-0100
beth@feganscott.com
megan@feganscott.com